Three-way security framework for cloud based IoT network

Zeeshan, Nida; Reed, Martin; Siddiqui, Dr. Zeeshan

Published in:
2019 International Conference on Computing, Electronics &amp; Communications Engineering (iCCECE)

DOI:
10.1109/iCCECE46942.2019.8941877

Published: 26/12/2019

Document Version
Peer reviewed version

Three-way Security Framework for Cloud based IoT Network

Nida Zeeshan[1], Martin Reed[1], Zeeshan Siddiqui[2] (Member, IEEE)

[1]*School of Computer Science and Electronic Engineering*
University of Essex Colchester, UK
{nz18123,mjreed}@essex.ac.uk

[2]*School of Computing, Engineering and Physical Science*
University of the West of Scotland, Scotland, UK
zeeshan.siddiqui@uws.ac.uk

***Abstract*—Internet of Things (IoT) is an extensive and rapidly growing technology in this modern era. Due to its networking nature and rapid implementation in various fields, security is considered a primary challenge. Due to various security vulnerabilities, IoT infrastructure is prone to numerous security threats which in return affecting the IoT infrastructure on a wider scale. This paper proposes a stronger and robust, three-way security framework which is based on Public Key Infrastructure (PKI) certification mechanism. This framework represents a unique way to authenticate both, IoT device and user using digital certificates before granting them access into the system.**

Keywords—information security, authentication, cloud computing, PKI, IoT security, IoT network, digital certificate

I. Introduction

Internet of things or widely known as IoT is increasingly becoming an undeniable part of our everyday lives. IoT is an advanced technology in which various everyday devices (things) are connected through gateways and various services. Most IoT devices can process and communicate over internet and contains Internet protocol address known as IP address. As illustrated in Figure 1.0, user can remotely access and control these IoT devices using existing framework which permits its integration with the modern-day rapidly growing world. The use of smart devices in an IoT infrastructure reduce the human interaction and make the daily life easier. [1][1]

The concept of smart environments and platforms like smart-city, smart-home and smart transportation has added a more innovative touch in everyday lifestyle. These innovations involve transfer of sensitive data related to a user or a device that requires sufficient security solution. These security solutions are required to build over a secure communication channel on the internet and should be able to overcome the concerns like authentication, availability and usability. Most of the IoT devices follow design patterns of cloud computing, such as, smart-home, where devices at every end are connected to cloud component via a local gateway [2]. Users can communicate and use IoT devices via this cloud component. This cloud component can store user token on behalf of its user name and password and allow user to communicate securely over a secure internet channel. A mobile application can be used as a security broadcaster through which user can authenticate and authorised certain IoT devices. This scenario increases security issues because cloud and the IoT devices transfer sensitive data of a user and can interact with the untrusted users which can harm authorised user's cloud component account [3].

Additionally, modern day Smartphones are considered an important component in IoT smart environment because it is used to communicate with both IoT devices and the cloud component [4]. In this research work, we have anticipated a framework which is offering a highly secure digital authentication for a normal user which enables user to communicate with IoT device via a cloud over a secure internet channel. The proposed framework is based on Public Key Infrastructure (PKI) that allow cloud and user to communicate and gain access to the restricted cloud services. In this paper, we proposed a new PKI-like security framework. This framework can provide user and device authentication where only a genuine user can use a registered IoT device. This framework is divided into two part. In first part IoT device and user will be registered with the cloud and in the second part user can use IoT device after authentication from the cloud.

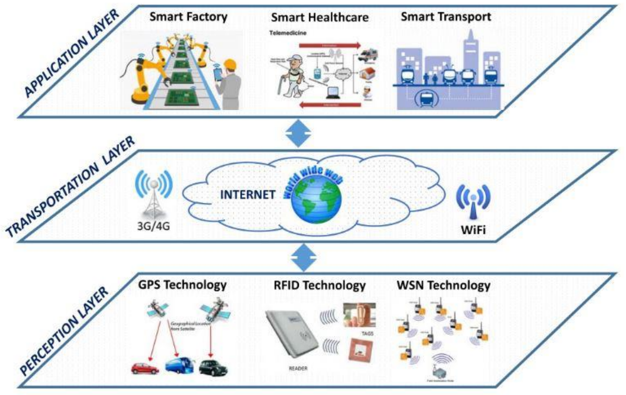

Figure 1.0. Generalized IoT Framework [5]

II. Background study

A. Internet of Thing

Internet-of-Things, or IoT, is considered the trendiest considered technology these days. This is becoming well-spread and well-organized industry of modern-day information technology infrastructure. It is in high demand and people are changing their lifestyle by adopting IoT technology. Although, the growth of this technology is fast-paced, however, at the same time it has encountered several security issues such as access control, intrusion detection and user authentication. Based on various studies, these security risks were not being considered one of the primary concerns and were not handled appropriately. Few of the major development to solve these security issues are encryption mechanism or cryptography, authentication mechanism and access control technology. [6]

B. Public Key Infrastructure (PKI)

PKI is an efficient approach to encrypt/decrypt the data. It gives us facility to securely and confidentially exchange data over an insecure environment such as IoT. PKI is widely known due to its use of pair of keys known as Public Key and a Private Key. These keys are related and derived from the same key-store. One key is used for encryption and other is used to decrypt that message. If Public key is compromised, the retrieval of Private key is not computationally possible. [7]

Implementation of PKI in IoT and Smart homes can be more feasible. Devices can encrypt data using a unique public key incorporated with a private key, which is used to decrypt the data at user's end. PKI digital certificate can also be useful to authenticate user and the devices that allow secure data transfer. Implementing PKI in IoT system is a big challenge because the procedure of encryption with public key requires the use of resources related to memory and existing wireless sensing technology do not facilitate this usage when transmission of data is frequently required. User and device authentication are also a major problem in this scenario. Communication with the cloud requires frequent authentication, it also increases few more issues such as, registration of a new user and devices. When these new devices transmit data, the device need permission to access to the public key to encrypt data. This also raise one of the primary issues which is Key Distribution issue. The communication between IoT device and the cloud need to be secure. [7]

A general PKI Digital Certification is third party entity that issues certificate after legitimate authentication. These authorities are known as CA (Certification Authority) which generate, issues and sign a digital certificate. RA (Registration Authority) which verifies the identity of the bodies requesting digital certificates to issue from CA, and a central management mechanism that is used to store and index certificate keys manage to control access to stored digital certificates. [7]

We proposed much secure framework using PKI digital certificate mechanism. This framework is based on three-way communication between user, IoT device and cloud. In this framework, cloud authenticate both user and IoT device using their digital certificate by the CA. User cannot communicate directly with the IoT device and without authentication. User must pass through gateway in order to communicate an IoT device.

C. Cloud Computing

Cloud Computing infrastructure is more convenient way of providing computing resources for shared group for example, networks, services, servers, and storage applications. Cloud services can provide fundamental necessities for PKI encryption, decryption and key management. [8]

D. Authentication

Internet of Things (IoT) is now becoming a part of our daily lives. It ranges from smart homes to wearable devices and implementation of IoT technology in healthcare. These implementations involve large amount of user's private data transfer. This increases the security concern. This includes authentication, data integration and access control and privacy. In main, the authentication of users and IoT devices has more importance to make the infrastructure secure. [9]

III. Literature Review

In term of security authentication of IoT devices is considered very important step. Privacy and security are the main problem in IoT devices. These devices must not be vulnerable to different types of attacks. Whitefield Diffie and Martin Hellman introduced Asymmetric cryptography or public key cryptography. It is one of the components which allow secure communication for different protocol such as, SSH, OpenPGP, HTTPS. These protocols are used in browsers, mobile and desktop applications and enabled secure connection on internet.

In the paper [7], authors have highlighted this issue in their proposed study. They use digital signature and device capabilities to authenticate an IoT device. Device only be allowed to use in when it is effectively authenticated over multifactor authentication, if not, the authentication procedure restart again.

In another study [10], authors have proposed a solution which is based on smart-card and three-factor remote user authentication protocol that can resist DoS attacks. It performs authentication by verifying the identity and password.

Various privacy and authentication issues have been discussed in [11]. The authors provided different authentication schemes using multi criteria classification that analyse the existing protocol.

In another relevant study [9], authors have highlighted the miss-use of user's private data that is being used on IoT devices and proposed a solution using object authentication.

In the paper [12], authors have highlighted several of the securities and vulnerabilities that exist in a layered architecture of an IoT infrastructure. According to the authors, the most susceptible layer is considered to be the application layer which fails to provide authentication, authorization, prototyping, validation, and availability.

In another relevant study [5], authors have analyzed various layered architectures of an IoT layered framework. They highlighted security vulnerabilities within three primary IoT layers; Perception, Transportation, and Application. Authors highlighted several threats on these layers, such as, Physical Attacks, Impersonation Attacks, DoS Attacks, Data Leakage, Malicious Code Injections etc. They also highlighted several communication levels of attacks in IoT protocols. The study was concluded while summarizing critical security issues and future directions for researchers.

Another survey-based study was carried out [13] in 2016. The study highlighted several security challenges in various IoT networks. They highlighted several security challenges related to Architecture Dependencies, Big Data, Robustness, and Privacy. The authors also highlighted the basic requirements of IoT while addressing security and privacy. Primary issues in authentication and access control were also highlighted such as, security protocols in IoT Cryptosystems, Security Vulnerabilities in IoT Software, OS level of Security issues, and Network level authentication challenges.

A reference architecture has been presented in [14] while highlighting security and business challenges in an IoT infrastructure for E-Commerce. Authors emphasized on several IoT challenges such as, Data Privacy, Data Security, Common Standard Shortcomings, Technical Limitations, and Social Concerns. A reference architecture was later on presented while focusing on Business Opportunities and IoT adaptable trends.

Based on the summarized review of various IoT based studies, in which several architectures, layers and frameworks for IoT has been discussed. It is pertinent that modern-day IoT networks are facing various challenges in almost all of their functional layers. However, based on the above discussion, the most prominent and threating security vulnerabilities exists on the application layer of the IoT infrastructure. As discussed and highlighted, application layer is defenseless against various threats such as impersonation, DoS, Malicious Code Injections, Cryptosystems vulnerabilities, Data Privacy, and other authentication and authorization threats.

IV. Proposed Study

As discussed in the literature review, various studies have addressed security issues, however due to the lack of emphasis on a more structured and robust security architecture, security and privacy issues are still at-large. Based on this understanding, authentication of IoT devices, access control, intrusion attacks are the major security issues one can face when implementing IoT system. In our proposed framework, we have focused on these security issues and proposed a secure framework which can provide a facility to register an IoT device using Digital Certificate as well as user to the cloud server. After completing registration process, only a genuine, registered user can only have access to use an IoT device available in the network.

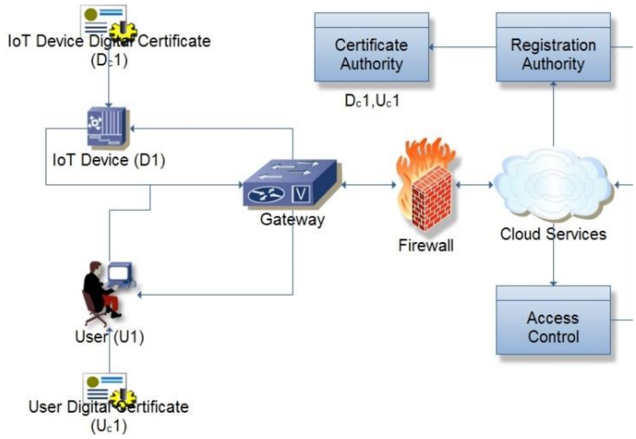

Figure. 2.0. Three-way Security Framework for Cloud based IoT Network

As illustrated in Fig. 2.0, the proposed framework is at its preliminary stage. The framework is based on PKI system that manages certificates, systems and application to uniquely identify users, services and devices that are being used in a network. An efficient PKI should be transparent and able to achieve security principles, specially authentication and data integrity. This framework consists of IoT devices, users, cloud, certification authority and registration authority. Before communication with each other, users and IoT devices need to be registered to the cloud through their verified Digital Certificate by the RA. Certification Authority further issues separate certificate for device and for users these certificates are represented as (D1, D2, … Dn) and (U_c1, U_c2, …U_cn) simultaneously. Third and most important entity in this framework is a centralized cloud, which stores and indexes all the certificates with their respective keys (D_c1, D_c2, … or U_c1, U_c2, … U_cn) in its centralized storage. Registration authority verifies each certificate issued by CA, and grant access to those entities that requires access to the system in order to access any IoT device.

When a user register, RA verifies its identity before allowing to store certificate in the centralized cloud. When a device register, RA verifies its identity and then store certificate in the centralized cloud. The cloud stores and index all the keys used to issue a certificate and the devices information. When the user wishes to use the device, RA verifies information about its certificate from the cloud and check the access control which is defined in the management system.

Public key certificates have the following services:

It contains repository for certificates, creation and revocation of certificate and management of key histories. It also contains key backup and recovery and backing for non-repudiation of digital signatures and automatic update of key pairs and certificates. These digital certificates include information such as public key, name, and expiry date of the certificate. Certification authority represents the most critical part in PKI. It acts as a source of trust and provide services to assure an individual level of authenticity to the entities when exchanging information.

The proposed security framework is expected to be robust and highly secure as it has covered the primary gap that exist on the application layer of an IoT infrastructure. Upcoming and extended studies based on our proposed work is going to provide a verifiable implementation of our proposed work. Table 1.0 has listed the abbriviations which are used to describe entities in our proposed framework.

TABLE I.

	Abbreviations
CA	Certification Authority
RA	Registration Authority
D1	IoT Device 1
D2	IoT Device 2
Dc1	Digital Certificate of device 1

	Abbreviations
U1	User 1
Uc1	Digital Certificate of User 1
IoT	Internet of Things
PKI	Public Key Infrastructure

V. Conclusion

In this paper we have presented a new secure and robust security framework which is based on PKI infrastructure and implemented on IoT network. As compared to previous and recent studies, this paper presented a more focused research based on security and authentication. As pointed-out earlier, the proposed Three-way IoT Authentication Framework is at its preliminary development stage. In our upcoming studies, we are aiming to present several detailed frameworks divided into various authentication phases and authentication protocols with sufficient results and outcomes to verify and validate out proposed work.

VI. Acknowledgment

The work was carried out within the project *SerIoT*, which has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 780139.

References

[1] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic iot networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, 2017.

[2] M. Togan, B.-C. Chifor, I. Florea, and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2017, pp. 1–7.

[3] N. Zeeshan, "WMW: A Secure, Web based Middleware for C4I Interoperable Applications," 2017.

[4] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: three factor cloud based user authentication for telecare medical information system," *J. Med. Syst.*, vol. 38, no. 1, p. 9997, 2014.

[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, 2018.

[6] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, "Enabling data protection through PKI encryption in IoT m-Health devices," in *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)*, 2012, pp. 25–29.

[7] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures," in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, 2018, pp. 1–5.

[8] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Comput. Stand. Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[9] K. Verma and N. Jain, "IoT Object Authentication for Cyber Security: Securing Internet with Artificial intelligence," in *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2018, pp. 1–3.

[10] J. Cui, Z. Zhang, H. Li, and R. Sui, "An Improved User Authentication Protocol for IoT," in *2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2018, pp. 59–593.

[11] M. El-Hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," in *2017 1st Cyber Security in Networking Conference (CSNet)*, 2017, pp. 1–3.

[12] B. V. S. Krishna and T. Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 107–111.

[13] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 2016, pp. 315–318.

[14] S. Singh and N. Singh, "Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1577–1581.